

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/802,931	03/12/2001	Inge Liden	Q63553	7226

7590 08/25/2004

SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20037-3213

EXAMINER

TRUONG, THANHNGA B

ART UNIT PAPER NUMBER

2135

DATE MAILED: 08/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/802,931

Applicant(s)

LIDEN ET AL.

Examiner

Thanhnga Truong

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 March 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 12 March 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 5/07/01.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-12 are rejected under 35 U.S.C. 102(b) as being anticipated by Uemura et al (US 4,912,310 B1).

a. Referring to claim 1:

i. Uemura teaches:

(1) creating a first user device having an electronic circuitry, creating a first system device having an electronic circuitry and being used in a first level of a lock system, storing a first encryption key in said first user device and said first system device, carrying out an authentication process between said first user device and said first system device using said first encryption key **[i.e. Uemura's invention provides a method of issuing cards by using a card issuing machine including a memory having stored therein an initial secret code, a card reader and a keyboard, the method being characterized by checking whether a secret code keyed in matches the initial secret code stored in the memory; storing in a memory a code keyed in for associating a first card with the card issuing machine and recording the associating keyed-in code in the first card by the card reader to issue the first card when the two secret codes are found to match; issuing a new card upon confirming a keyed-in first secret code of the first card; and issuing another new card upon confirming a secret code of the new card issued (column 2, lines 55-68)],** and

(2) in case said authentication process was successful, carrying out a software operation by said first system device, by which software

operation said first encryption key stored in said first user device is replaced' by a second encryption key [i.e., **the first card is issued by the card issuing machine on condition that the secret code keyed-in matches the initial secret code stored in the memory of the machine. At this time, a code for associating the first card with the card issuing machine is keyed in and stored in the first card and in the machine. With the issue of the first card, the first card is closely associated with the issuing machine. The first card is of the highest level and serves as a key for issuing another card of lower level (column 3, lines 10-18)],**

(3) wherein said second encryption key is stored in second system devices and user devices used in a second level of said lock System, thereby making said first user device operable with said second system and user devices [i.e., **a second secret code as to the second card is similarly stored in the card or in the card issuing machine (column 3, lines 31-32)].**

b. Referring to claim 2:

i. Uemura further teaches:

(1) wherein during the step of replacing said first encryption key stored in said first user device, said second encryption key is supplied by said first system device [i.e., **the second card can be issued on condition that a secret code keyed in matches the first secret code stored in the card issuing machine. Accordingly, the second card can not be issued by those other than the registerer of the first secret code (column 3, lines 26-31). Uemura's invention further provides a card issuing system which is characterized in that the system comprises a card reader for reading card data from a first card, a keyboard for entering a secret code of the first card and data needed for issuing a second card, means for checking a secret code keyed in with the secret code in the card data read from the first card by the card reader or with a secret code accessible by the card data in the first card, a card writer for issuing the second card, and means for controlling the card writer so that when the two secret codes are found to match, specified card data including the keyed-in data is written in the second card by the card writer (column 3, lines 49-61)].**

c. Referring to claim 3:

i. This claim has limitations that is similar to those of claim 2, thus it is rejected with the same rationale applied against claim 2 above.

d. Referring to claim 4:

i. Uemura further teaches:

(1) comprising the additional step of supplying said second encryption key to said computer through a network including local networks and public telephone networks [i.e., **card issuing consoles include a parent machine 10 and one or a plurality of satellite machines 11 connected thereto by transmission cables (column 5, lines 40-42).**]

e. Referring to claim 5:

i. Uemura further teaches:

(1) wherein said first system device is a system key of a master key system [i.e., **Figure 2 shows the kinds of cards to be used for the hotel card lock system and the security levels thereof. A grand authorization card (hereinafter abbreviated as a "GR card", that is "system key") is the highest in security level (grand level). This card is to serve as a "key" for the overall system. The cards of the second highest level (authorization level) are a master authorization card, sub-master authorization card and guest authorization card (hereinafter referred to briefly as "MA card," "SMA card" and "GA card," respectively). These three kinds of cards, that is "system key", at the authorization level correspond to the authorization cards AC shown in Figure 1. (column 6, lines 2-14).**]

f. Referring to claim 6:

i. Uemura further teaches:

(1) wherein said first user device is a user key of a master key system [i.e., **the level for unlocking the hotel room (unlocking level) is divided into management level, guest level and maintenance level. Available at the management level are an emergency card, master card and maid card. The cards at the guest level are a standby card, guest card A and guest card B. The**

cards at the maintenance level are a maintenance card, lockout card and cancelling card. These nine kinds of cards at the unlocking level correspond to the key cards KC, that is “user key”, shown in Figure 1 (column 6, lines 15-23)].

g. Referring to claim 7:

i. Uemura further teaches:

(1) wherein said first user device is a lock of a master key system [i.e., a card lock unit 70 includes a card reader for reading data from the key card KC. The card data is checked before unlocking (column 5, lines 53-55)].

h. Referring to claim 8:

i. Uemura further teaches:

(1) wherein said electronic encryption keys are unreadable from outside said electronic circuitry [i.e., this check is specific to the guest cards A and B. The guest card data includes date of issue of the card (check-in date) and check-out time. When the present time minus the allowable check-out overtime is between the day of check-in and the check-out day, time, the card is acceptable. Otherwise, the card is judged as being invalid, that is “unreadable” (column 29, lines 40-47)].

i. Referring to claim 9:

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

ii. Uemura further teaches:

(1) an electronic circuitry having an electronic memory adapted for storing an electronic code, said electronic code uniquely identifying the device and comprising a first electronic encryption key [i.e., Figure 6 schematically shows the electrical construction of the card issuing console (parent machine) 10. The console 10 includes a control unit 20 comprising a central processing unit (CPU), a ROM having stored therein the program to be executed by the CPU and other fixed data, and a RAM for storing variable data. Connected to the control unit 20 through a suitable interface are the foregoing ten-key arrangement 16, function switches 15, display 12, totalling printer 11, satellite connector 23

and data input unit connector 24, and further a card reader 21 and a card reader 22 with a printer (column 9, line 64 through column 10, line 8)].

j. Referring to claim 10:

i. This claim has limitations that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

k. Referring to claim 11:

i. This claim has limitations that is similar to those of claim 7, thus it is rejected with the same rationale applied against claim 7 above.

l. Referring to claim 12:

i. This claim has limitations that is similar to those of claims 1-7 and 9, thus it is rejected with the same rationale applied against claims 1-7 and 9 above.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Cregger et al (US 6, 384, 711 B1) discloses an electronic security system includes an electronic lock mechanism and an electronic key, each of which is provided with a microprocessor controller and a memory storing data including an ID code and encryption key codes (see abstract).

b. Nendell et al (US 6, 343, 361 B1) discloses Methods and systems for verifying and authenticating the identity of participants in electronic communication. The identity of a recipient communication device, such as a computer, can be verified. A primary key generated from a master key is stored at a sending device and the recipient device (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and


Art Unit: 2135

phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT

August 19, 2004



KIM VU
ASSISTANT PATENT EXAMINER
TECHNOLOGY CENTER 2100